Commonwealth of Kentucky
Public Protection Cabinet

**Steve Beshear, Governor** **Larry R. Bond, Acting Secretary**

**FOR IMMEDIATE RELEASE**

**Contact: Kelly May**
**502-782-9031 Direct**
**502-229-5068 Cell**
**kelly.may@ky.gov**

# Beware of 'Shellshock' Phishing, Apply Patches to Software

*Cybercrime Task Force Urges Institutions, Consumers to Be Alert*

**FRANKFORT, Ky. (Sept. 30, 2014) –** Today the Financial Cybercrime Task Force of Kentucky – a work group of the Department of Financial Institutions (DFI) – alerted the financial services industry about a software vulnerability known as "Shellshock."

The Task Force also urges businesses and consumers to apply patches to software as they become available and to be wary of phishing attempts.

Shellshock is a material security vulnerability in the Bourne-again shell (Bash) system software. Bash is found predominantly on UNIX, Linux and Mac systems, although it can also be installed on Windows servers. Bash is used to translate user instructions and other inputs into machine-readable commands. The Shellshock vulnerability, reported to be in Bash versions 1.14 through 4.3, could allow a remote attacker to run malware on affected systems.

"When security vulnerabilities make the news, there are often con artists who will base a scam around it," said DFI Commissioner Charles Vice. "Guard against phishing by avoiding links in emails you did not request and dealing only with websites and companies you trust."

People should be wary of links in email notices as these could be phishing attempts. Phishing is the use of fraudulent email to acquire sensitive information, such as passwords and financial account details. Phishing e-mails appear to be from legitimate sources, such as banks or online services. Often the link will lead to a false website that looks identical to the company's real site, luring the consumer to reveal logon credentials or other personal information to cybercriminals.

Also beware of other possible scams, such as services that offer to scan for and repair vulnerabilities on your computer. Research any service provider you plan on using to make sure it is a legitimate business before turning over any money or information.

In this instance, applying a patch when it becomes available from a known provider will be the best solution to the Shellshock vulnerability. Passwords should be changed after vulnerable systems have been patched.

DFI's alert (*#A0914-01)* can be found here: http://kfi.ky.gov/industry/Pages/cybercrime.aspx.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, http://kfi.ky.gov, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.

###